Strategy Research Project

Homeland Security and Homeland Defense: The Seam of Uncertainty Unstitched?

by

Lieutenant Colonel Harry Culclasure
United States Army

United States Army War College
Class of 2012

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 22-03-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Homeland Security and Homeland Defense: The Seam of Uncertainty Unstitched?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Harry Culclasure

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Mr. Bert Tussing
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Both the terrorist events of September 2001 and the natural disaster of Hurricane Katrina in 2005 have emphasized the need for a tiered capability toward all hazard response in the United States. The Department of Homeland Security (DHS) and United States Northern Command (USNORTHCOM) continue to improve capabilities and coordination with one another but still have gaps that lack clarity, affect response times, limit information sharing, and cause incident command confusion. This "seam of uncertainty" exists where the DoD homeland defense mission overlaps with DHS homeland security. The US dedicated itself to meet and close these seams to better prevent, prepare, respond, and recover from future events that challenge our response enterprise. What improvements are needed in the CBRNE Response Enterprise and National Response Framework to enhance our ability to respond and recover from natural and manmade disasters?

15. SUBJECT TERMS
CCMRF, CERFP, DCRF, HRF

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

HOMELAND SECURITY AND HOMELAND DEFENSE: THE SEAM OF UNCERTAINTY UNSTITCHED?

by

Lieutenant Colonel Harry Culclasure
United States Army

Mr. Bert Tussing
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Lieutenant Colonel Harry Culclasure
TITLE:	Homeland Security and Homeland Defense: The Seam of Uncertainty Unstitched?
FORMAT:	Strategy Research Project
DATE:	22 March 2012 WORD COUNT: 5,889 PAGES: 30
KEY TERMS:	CCMRF, CERFP, DCRF, HRF
CLASSIFICATION:	Unclassified

Both the terrorist events of September 2001 and the natural disaster of Hurricane Katrina in 2005 have emphasized the need for a tiered capability toward all hazard response in the United States. The Department of Homeland Security (DHS) and United States Northern Command (USNORTHCOM) continue to improve capabilities and coordination with one another but still have gaps that lack clarity, affect response times, limit information sharing, and cause incident command confusion. This "seam of uncertainty" exists where the DoD homeland defense mission overlaps with DHS homeland security.[1] The US dedicated itself to meet and close these seams to better prevent, prepare, respond, and recover from future events that challenge our response enterprise. What improvements are needed in the CBRNE Response Enterprise and National Response Framework to enhance our ability to respond and recover from natural and manmade disasters?

HOMELAND SECURITY AND HOMELAND DEFENSE: THE SEAM OF UNCERTAINTY UNSTITCHED?

> …we will not be able to deter or prevent every single threat. That is why we must also enhance our resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.
>
> —President Barack Obama[2]

Following the tragic events of September 11th the United States embarked on a series of efforts to combat terrorism, including the establishment of the Department of Homeland Security (DHS) in 2003 and the United States Northern Command in 2002. In 2005, Hurricane Katrina caused unprecedented damage across multiple state and local governments, challenged our emergency preparedness, and ultimately demonstrated how quickly our civilian and military first responders could be over-extended in large natural disasters. These two separate events became the focal response incidents on which to base our national response enterprise for the federal government. In the past ten years the government established or combined multiple agencies and vertical layers to improve our planning, execution, and recovery from disasters. The DoD, playing a supporting role in Defense Support of Civil Authorities (DSCA), also established a new command to assist in natural and man-made disasters. DSCA adds a second mission space apart from DoD's Homeland Defense mission and the protection of US sovereignty and territory. This paper intends to study the ends, ways, and means and identify shortcomings where the seams between Homeland Security and Homeland Defense become apparent in preventing, protecting, responding to, and recovering from natural and manmade disasters. Current strategic policies represent our desired ends; the policies' application represent the ways; and the agencies and units required to accomplish the CBRNE response mission represent the means. After reviewing the response enterprise from the top down the paper intends to identify the capability gaps that still remain in the enterprise and make recommendations for their improvement.

The New York Example

As one of the most targeted cities for terrorism, New York City invested more than $3 billion dollars to address the terrorism threat and make it a difficult target for future acts. In a *60 Minutes* interview aired on 25 September 2011, Raymond Kelly, the New York Police Commissioner, reviewed the personnel, equipment, and tactics the city uses to deter and respond to emergencies. The city employs over 35,000 uniformed police officers, maintains well over 2,000 cameras, and uses swarming techniques to take over city blocks. It constantly monitors the harbor and vehicles entering the city with sensitive radiological detectors and software that recognizes potential hazards on the streets. To gather intelligence on emerging threats, the city employs linguists in sixty languages across the world.[3] These linguists report back to the city's counter-terrorism group, where their information is used to develop estimates on activities. Intercepted phone calls from potential terrorists have confirmed these techniques are effective. To date it appears the city's deterrence methods are working and would-be terrorists need to look elsewhere at less capable cities.

New York City stands as an example of how coordination, information sharing, and response units, when used together, close the seams between "prevent, prepare, respond and recover." NYC is one of the few cities in the US which commands a budget large enough to afford these capabilities, and can respond with little help from outside agencies. Other US cities and communities do not have the funds (or the constant terrorist threat), and will require assistance when man-made or natural disasters occur. For them, as suggested by New York's example, the answer is a multi-layered and partnered response. That answer is written throughout the documents discussed in this paper, but enacting the collaboration, information sharing, and capabilities of the players needed to execute that answer remains elusive.

The Ends: Interagency and Department of Defense Objectives for Emergency Response

The strategy for Homeland Security and Homeland Defense begins with national level objectives designed to communicate and promote collaboration within the government. These documents set the stage for combined strategy to protect the homeland and nest all the way down to the response level -- or means—contained in the civil and military components of our Nation's government.

The National Security Strategy (NSS) identifies threats at home in the United States that include terrorism, natural disasters, cyber-attacks, and pandemics.[4] It provides the federal government's objectives -- or ends -- based on current US priorities. The strategy calls for enhancing security at home and effectively managing emergencies through all levels of the government and the private sector. It calls for "individual and community preparedness and resilience through frequent engagement" that supplies clear information to the public.[5] As noted in the NSS, the US cannot expect to prevent or deter the potential damage caused by every terrorist plot or natural disaster.[6] To reduce an event's effect, the NSS calls for investment in preparedness throughout all levels of government to include planning, equipping, and information sharing and collaboration across all response elements.

To build upon the guidance in the NSS, President Obama issued *Presidential Policy Directive 8: National Preparedness,* which established the national preparedness system. The system allows the nation "to track the progress of our ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the Nation."[7] It looks into risks trends all over the Nation and "includes concrete, measureable, and prioritized objectives to mitigate the risk."[8] The risk data is placed in frameworks coordinated under a "unified system with common terminology" and built upon "basic plans that support an all-hazards approach to preparedness."[9]

As a supporting document to the National Security Strategy, the 2010 Quadrennial Homeland Security Review (QHSR) report effectively replaced the 2007 National Strategy for Homeland Security (NSHS). The QHSR was the first document to look at Homeland security as an "enterprise….the collective efforts and shared responsibilities of Federal, State, local tribal, territorial, non-governmental, and private sector partners- as well as individuals, families, and communities…."[10] It stresses homeland security missions are not solely the responsibility of DHS, but are "enterprise-wide" and everyone has the responsibility for executing HS missions.[11] It expands a focus frequently limited to response and recovery, to incorporate mitigation and preparedness.[12] This shift in direction requires less of a top down emergency management approach, and engages all stakeholders from the State down to local government, NGOs, private sector, communities, and individuals.[13] At the core of response is the use of the National Response Framework (NRF) and the National Incident Management System (NIMS) which provide roles, responsibilities, and effective response mechanisms during disasters.

There are numerous gaps between local, state and federal governments (to include DoD) pertaining to information sharing and protocols needed to improve situational awareness during an incident. The QHSR addresses these shortfalls and calls for "greater real-time shared threat information and situational awareness….avoid[ing] stovepipes that hinder appropriate information sharing and analysis…."[14] Additionally, it recognizes that in order to share information the entire homeland security enterprise "must use compatible information architecture and data standards" which avoids duplication and enhances preparedness.[15]

Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, tasked the Secretary of Homeland Security to develop the National Incident Management System (NIMS) to close the gaps between federal, state and local entities. The objective was to "provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity."[16] It solidified the DoD's support to civil authorities and tasked the Secretary of Defense and Secretary of Homeland Security to establish "appropriate relationships and mechanisms for cooperation and coordination between their two departments."[17] HSPD-5 also established the National Response Plan (NRP), updated as the National Response Framework (NRF), and defined the roles and responsibilities of government in terms of an "all hazards" plan. These two documents, the NIMS and the NRF, are the synthesis to provide a unity of effort between the military and the civilian sector. The relationship and coordination between DoD and the rest of the Interagency is crucial to response, and is emphasized in the 2010 QHSR. It stresses the need to "strengthen unity of effort between military and civilian activities….and revise strategy and doctrine accordingly."[18] The 2010 QHSR was the first document to place a strong emphasis on this relationship and call for a unity of effort for disaster response from Federal, State, and local levels.

The DoD Quadrennial Defense Review (QDR) report emphasizes DoD contribution in Defense Support of Civil Authorities (DSCA), a role that "has steadily gained prominence."[19] It explains the Department's role in DSCA, in support of the Department of Homeland Security as the lead federal agency, and/or in support of a governor's request under Title 32.[20] The QDR reviewed the force capabilities and identified areas where DoD could most affect the DSCA mission. Among the recommendations that emerged from the review was a call for more capable CBRNE Consequence Management Response Forces (CCMRF). The CCMRF is a Title 10 force consisting of 4,700 soldiers in three brigade sized units -- two from the National Guard and one from the Active component -- with operations, aviation, medical and other specialized units. Its primary mission is to "augment the consequence management efforts of the first responders."[21]

The QDR directed the reorganization of the CBRNE Response Enterprise. The CCMRF that had been stood up prior to the QDR's direction effectively became three units: the Defense CBRN Response Force (DCRF) and the two Command and Control CBRN Response Elements (C2CRE). Plans for the two National Guard CCMRFs were replaced with what have become ten Homeland Response Force (HRF) units, each aligned with a FEMA region. DoD introduced all of these changes in order to create a more flexible force with quicker response times, and to increase its ability to respond to simultaneous events. This new structure intends to capitalize on planning and coordination with FEMA in each of the regions.

The DoD and the rest of the Interagency produced clear guidance in the documents discussed and targeted similar ends to construct a layered approach to protect the homeland. For the Interagency to succeed in prevention, protection, mitigation, response, and recovery, it requires a forcing function to provide the whole of government response. The Goldwater-Nichols Act achieved “jointness” in the military; a similar act could assist the rest of the Interagency.

The Ways: The Interagency Application of the Means

DHS began operations in 2003 with the mission to prevent terrorist attacks, reduce our vulnerability, and minimize the damage if an attack occurs.[22] In the past ten years DHS grew to the third largest federal government agency with over 200,000 employees and $50 billion dollar budget. As previously noted, HSPD-5 tasked DHS to develop the National Incident Management System (NIMS) and the National Response Plan, which evolved to become the National Response Framework.

The NIMS provides a proactive approach to organize the government, Non-Governmental Organizations (NGOs), and the private sector to respond to and recover from disasters. It is based on the premise that the use of a common “incident management framework” will give emergency management/response personnel a flexible but standardized system for emergency management and incident response activities.”[23] The system is based on five components: preparedness, communications and information management, resource management, command and management, and management and maintenance. The components concentrate on the ability to manage emergency personnel and equipment, maintain a common operating picture and interoperability, manage resources, and maintain command structure. It strives to produce a unified command where all players in a disaster work seamlessly toward a common goal to reduce the loss of life and property. The NIMS makes it clear that it is neither a response nor a communications plan, but a "comprehensive, nationwide, systematic approach to incident management, including the incident command system, multi-agency coordination systems, and public information."[24]

The National Response Framework (NRF), a companion document to the NIMS, "is a guide to how the Nation conducts all hazard response…built upon scalable, flexible and adaptable coordinating structures to align key roles and responsibilities across the nation."[25] To coordinate response and provide support, the Federal Emergency Management Agency (FEMA) organized its response capability into 15 Emergency Support Functions (ESF), such as firefighting, communications and transportation. The ESFs "bundle and funnel resources and capabilities to local, tribal, State, and other responders."[26] The application of the ESFs helps provide organized support to communities in need.

DoD produced three joint documents related to its Homeland Defense / Civil Support mission in the 2006-2007 timeframe. Joint Publications 3-27, 3-28, and 3-41 each explain the critical missions tasked to the Department in Homeland Defense and Civil Support. All three reference the strategic documents mentioned earlier in this paper, and DoD's relationship to Homeland Security. They explain DoD's "place" in NRF and NIMS, and under what authorities it responds to crises in the homeland.

Joint Publication 3-27, *Homeland Defense*, gives an overall view of the HD mission but also explains the relationships with other agencies in the government to achieve mission success. It acknowledges the communication gaps during the events of 9-11 and stresses the transition from a "'need to know' to a 'need to share' culture."[27] In JP 3-28, *Civil Support*, DoD explains the mission of Civil Support, the Request for Assistance (RFA) process, and the roles of Title 10 and Title 32 forces in the homeland, informed by lessons learned from Hurricane Katrina. It reinforces the need to share information during a disaster because "information sharing and the interaction with agency liaison personnel prior to and during CS exercises and operations significantly enhance real-time information sharing and coordination activities and improve CS related response capabilities."[28] Finally, JP 3-41, *Chemical, Biological, Radiological Nuclear and High-Yield Explosives Consequence Management*, takes a close look at the CBRNE response capabilities in DoD. The publication challenges its commanders and staffs to understand the NRF and the NIMS, and know where their units fit in the overall response framework.[29] The document educates DoD members on the formation of the Joint Field Office where officials work to achieve unity of effort when dealing with a threat or hazard.

The three DoD documents discussed in this section give a clear guidance on the varying missions under Homeland Defense and Civil Support. Each uses the nation's strategic documents and reiterates the necessity to understand the NIMS and NRP and where DoD fits in it. Finally, they take the lessons learned from 9-11 and Hurricane Katrina to reinforce the need to share information across the response enterprise.

The Means: DoD and DHS Resources in the Response Enterprise

DHS and DoD work together during a domestic incident through the Federal Emergency Management Agency (FEMA) and the United States Northern Command (USNORTHCOM). USNORTHCOM is responsible for the CBRNE Response Enterprise and supports the Primary Federal Agency in the event of a CBRNE event. It responds to Requests for Assistance (RFA) according to the NRF when directed by the President or the Secretary of Defense. FEMA is responsible for coordinating federal response to disasters. Both USNORTHCOM and FEMA use the NIMS and the NRF to coordinate support for incident response. This section will explore the roles and responsibilities of each and the resources available to respond and recover from incidents.

FEMA became a part of DHS in 2003 with the mission to "support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards."[30] With roughly 7,500 employees in 10 Regions throughout the United States, FEMA acknowledges it is not the "the team, but part of a team" that includes federal partners, state and local officials, and the private sector.[31]

To meet the demands for incident response, FEMA organized itself into the aforementioned regions to integrate disaster preparedness, incident management, emergency communications, and logistics. They rely upon existing community emergency response personnel and combine them into teams to respond to an event. These teams include capabilities such as Urban Search and Rescue and mobile communications to affected communities. The FEMA employees report to Regional Response Coordination Centers (RRCC). In the event of an emergency FEMA coordination is accomplished through the Joint Field Office (JFO) which coordinates all disaster response.

The direction of the DoD response enterprise changed in 2010 with the Quadrennial Defense Review. Prior to 2010 the enterprise basically consisted of the

National Guard Weapons of Mass Destruction Civil Support Teams (WMD CST) and the CBRNE Enhanced Response Force Packages (CERFP). Three CBRNE Consequence Management Response Force (CCMRF) packages had been planned for: two from the Guard and one from the Active Component. As previously alluded to, only one CCMRF unit was ever stood up; plans for the other two were abandoned with the QDR's objectives.

To increase its ability to respond more quickly to disasters the QDR instructed DoD to restructure the CBRN Enterprise, with a particular focus on lifesaving capability, flexibility, and response times."[32] This direction resulted in the development of ten Homeland Response Forces (one in each FEMA region); a Defense CBRN Response Force; and two Command and Control CBRN Response Elements (C2CRE). The envisioned response time improved with the HRF response to no later than N+12, as compared to the old CCMRF at N+48.[33] The HRF's positioning in their respective FEMA region, under the governor's control, places them in a better geographical location to respond to crises. They are not as large as the prior mentioned CCMRF units. On the other hand their dispersed locations allow them an opportunity to work and train with FEMA thereby increasing their awareness and response time. All ten HRFs are currently manned and undergoing certification.

The CBRNE Response Enterprise actually began with the Civil Support Teams (CSTs). There are currently 57 CSTs with at least one in each the states and territories (there are two each in New York, Florida and California). The teams consist of 22 active Guard personnel serving under Title 32 authority. The teams respond to state and territorial governors for the identification and survey of suspected chemical, biological, and radiological events. The teams deploy within 3 hours of notification with a mobile laboratory and a communications vehicle capable of classified communications and some limited voice and data (internet) communications with civilian first responders.[34]

The next tier in the response enterprise is the NG CERFP. There are currently 17 units consisting of 186 personnel, with a small number of Title 32 members (normally less than 25%). Their mission is to conduct search and extraction, search and recovery, decontamination of affected personnel, and initial triage. CERFP units can deploy within 6 hours' notification.[35] Unlike the CSTs, the CERFP does not have a robust communications capability.

The Homeland Response Force (HRF) consists of 566 personnel in each FEMA region for a total of 5,660**.** The force maintains no more than 25% of its element in Title 32 status. Its mission is much like the CERFP; but it also contains a command and control element, security, and additional triage and treatment. The HRFs are required to deploy within 6-12 hours after notification.[36]

The CSTs, CERFPs, and HRFs are the first three echelons, other than civilian first responders, available to respond to a CBRN event. These elements remain under the command and control of a given state or territory's governor unless federalized. If the units respond to another state with the approval of the respective governor, the supported governor assumes tactical control of the unit.[37] This is accomplished through interstate agreements, the most notable of which is the Emergency Management Assistance Compact (EMAC). This mutual assistance agreement provides support to "any emergency disaster that is duly declared by the Governor of the affected state" and includes events such as "natural disaster, technological hazard, man-made disaster, civil emergency aspects of resources shortages, community disorders, insurgency, or enemy attack."[38] The EMAC is granted under public law by Congress.

The Defense CBRN Response Force (DCRF) and the Command and Control CBRN Response Elements (C2CRE) are the first Active Component response forces in the enterprise allocated to USNORTHCOM. The DCRF is primarily an active duty force but can contain Reserve and National Guard elements. It consists of 5,200 personnel: 2,100 in Force Package 1 (FP1) and 3,100 in Force Package 2 (FP2). FP 1 is required to deploy within 24 hours of notification and FP 2 within 48 hours. The DCRF is the first unit to bring rotary wing aircraft for patient evacuation, as well as level III medical care. The C2CRE A and B packages provide an additional 1,500 personnel from the Active and Reserve Forces. They have capability similar to the DCRF, but are composed of smaller units. National Guard CSTs, CERFPs, and HRFs from unaffected areas can be federalized to provide additional capability to the DCRF. The C2CRE is required to deploy in 96 hours.[39]

The events of 9-11 and the lessons learned from hurricanes and other natural disasters forced the Federal government to review its response enterprise to garner a more robust response. The United States now has a very capable, well trained, and equipped response force for disasters, but there are numerous limitations to its current configuration. These limitations include proposed response times, common operating pictures, and general knowledge of and between DHS and NORTHCOM. These themes are common throughout all the documents previously explored in this paper.

Limitations to the Response Enterprise

While the United States adjusted the size and locations of units responsible for emergencies, the most important traits are rapid response, life-saving capabilities, the ability to share information, and the capacity to make timely decisions during a crisis. This section explores some of the limitations in the processes and the response forces.

Military first responders such as the CSTs, CERFP, and HRF are controlled by the state governor, who in most cases, places them on State Active Duty (SAD) for response.   The CSTs are the only unit in the Guard on active duty for immediate response to a Chemical, Biological, Radiological and Nuclear event. The CERFP are the first to respond with lifesaving capabilities but have only 25 percent of their force on Title 32 status at any one time; only 45 of the 186 personnel are available for an unanticipated emergency event. This is not a criticism of the Guard or the training level of the CERFP, but one example of time factors that can limit response. The six hour assembly time for the CERFP, combined with the travel time to the incident site, is crucial when an unanticipated event occurs. This time lag limits the initial assessments sent to the governor, and adds more time to the decision making process if additional forces are needed for response.

The HRF is in a similar position. Even with a response capability within twelve hours, the HRF faces a shortcoming by only maintaining 25% of its personnel in Title 32 operational status.[40] The HRF cannot assemble and deploy until the governor places them in State Active Duty (SAD). In an unanticipated event the HRF has 141 personnel immediately available for response, and some of those may not be part of the lifesaving capability. Even with the quick assembly time for the HRF, they can still expect to travel up to 500 miles to the incident site. Multiple incidents in the same FEMA region or on state borders can cause even greater problems. Governors may hesitate to acknowledge an Emergency Management Assistance Compact (EMAC) as they assess the damage and danger to their particular state. All of these considerations add precious time to the lifesaving capability the CERFP deliver.

The DCRF faces a greater challenge in relation to time. Domestic response, as with all DSCA, is driven by the Request For Assistance (RFA) process from civil authorities.[41] The President or the SECDEF direct the response to an RFA. It is forwarded to USNORTHCOM in accordance with the National Response Framework to support a primary agency, e.g., FEMA.[42] Once USNORTHCOM receives the order it may take up to 24 hours for the DCRF to begin movement to the incident site. The availability of air transport and proximity to the incident play a large factor on the success of the response. The initial 96 hours after an event offer the greatest opportunity to save lives and poses one of the greatest challenges.[43] A USNORTHCOM CBRN Response Enterprise brief to its Senior Steering Group, dated 23 September 2011, emphasized the time involved in HRF and DCRF deployments. The brief called out the number one concern as "can we get there in time?"[44] To address the deployment timelines USNORTHCOM utilizes Deployment Readiness Exercises (DRE) as the key to measure a unit's ability to deploy and its installation's capability to support a deployment.[45]

The notion of time also permeates the decisions state, local, municipal, and tribal leadership consider during an emergency. After an incident occurs it is imperative the leadership in the community or state receives the best timely information to make informed decisions. According to the National Response Framework "incidents must be managed at the lowest possible jurisdictional level and supported by capabilities when needed."[46] Immediately following an unanticipated event the ability to receive accurate information can prove challenging. While the local authorities and first responders react to the event they may not know if the incident exceeds their capabilities. As the NRF states, "it is not always obvious at the outset whether a seemingly minor event might be the initial phase of a larger, rapidly growing threat."[47] Once the community requests assistance from the State more time is used to assess what resources are needed at the State level. If the Governor expects the incident to exceed the State's capability he/she may request assistance from other States via EMAC or other agreements. If the event overwhelms or is anticipated to overwhelm the State's capability, the Governor may request assistance from the Federal government. To request this assistance the governor can request assistance under the Stafford Disaster Relief Act. The Stafford Act authorizes the President to "provide financial and other assistance …certain private nonprofit organizations, and individuals to support response, recovery, and mitigation efforts".[48]

Most events do not warrant the use of a Presidential declaration, but when necessary the governor must ensure all state functions are potentially overwhelmed and issue a formal request to the President. The governor's request for a Presidential declaration must include a survey of the area, a joint damage assessment with FEMA, and a consultation with the regional FEMA administrator for eligibility.[49] This process takes up precious time needed to activate response forces and for them to move to the incident site.

The NRF does allow for a proactive response to unanticipated events, such as CBRNE threats, that can cause catastrophic loss of life and property. The NRF provides an ability to pre-position Federal assets "in anticipation of a formal request from the State for Federal assistance," allowing for a proactive means to provide support.[50] The notion of a proactive response makes the need for information sharing even more important. There are too many time variables involved in domestic response from the local to state to federal which depend upon accurate, timely information. A local government can quickly become overwhelmed in an incident which then adds time to the state and additional time to the Federal response. These times only improve when the whole of government shares intelligence and response information in the form of a Common Operating Picture (COP), the "overview of an incident created by collating and gathering information…. from agencies/organizations in order to support decisionmaking."[51]

The 2010 Quadrennial Homeland Security Review report (QHSR) underscores the necessity to shorten the information sharing process through the entire enterprise, and not just within the Department of Homeland Security. It stresses the need to "avoid stovepipes that hinder appropriate information sharing and analysis, and foster greater information sharing"….from a "top-down command and control model to a more bottom-up approach."[52] Information sharing throughout the enterprise can unquestionably improve response times from the local, to the state, and up to the Federal level. While the solution is easily recognized, achieving the end state is much more complicated. Gaps still exist within the intelligence community and DHS due to an inability to supply a single enterprise information system that meets the requirements for all.

The enterprise suffers from several factors that inhibit its information sharing and networking. Security clearances, over classification, and governance issues, all contribute to a lack of integration and interoperability. For the enterprise to truly be responsive it requires the ability to access and share information not just vertically but horizontally.

One of the most critical factors that hamper information sharing in the intelligence community is the governance issue. DHS as it operates now "is poorly positioned to receive intelligence from the intelligence community agencies because it does not do intelligence collection on its own."[53] Without political support from the Congress and control of a budget, the Director of National Intelligence (DNI) cannot break down the stove pipes and the resistance to reform that exists in the intelligence communities.[54] No one in the intelligence community has the ability to collect and process all the available information into actionable intelligence.[55] To remedy this shortfall and transform the community the DNI needs to establish a new community based on collaboration and abolish the current rivalries. The Goldwater-Nichols Act of 1986 is an example of reform that streamlined the command structure within DoD. It created a "unified military establishment and, among other things, laid the foundations for a 'joint' military."[56] A similar act from the Congress could establish a more collective intelligence environment. The act could break down the barriers of the "need to know" culture past the "need to share" and into a mindset of "responsibility to provide".[57] These communities need to overcome past biases and provide threat information across the enterprise while protecting the source.

Before any intelligence is provided the community must also confront security clearance issues. There is an "inability or unwillingness on the part of DHS and FBI to work effectively together" on this issue.[58] Many states and some major metropolitan areas maintain fusion centers, a central repository on intelligence mainly tied to law enforcement, with “a higher degree of vertical (federal intelligence community) and horizontal (state/local) collaboration.”[59] These fusion center operators require security clearances to receive, analyze, store, and disseminate this classified information. There are reported cases where the FBI did not accept DHS security clearances; and others where DHS required verification from fusion centers that personnel possessed an FBI clearance, certified to DHS from the FBI.[60] These occurrences frustrate the state fusion centers, which are not funded through federal dollars but by the individual states.

Even if the fusion center personnel receive the clearances, a problem still exists with the over-classification of intelligence. The Interagency lacks an overarching policy on Sensitive but Unclassified (SBU) documents, which doubled since 2001, and procedures that deal with the designation of these documents.[61] The SBU documents are of “particular importance to homeland security,” but the designations are “misapplied and disjointed.”[62] This lack of understanding on classifying material is a serious impediment to sharing information. According to the 2006 Government Accountability Office (GAO) report 06-385, the government used fifty-six different SBU designations and applied them on information that did not warrant classification.[63] This misuse of classification denies state and local fusion centers the ability to act on intelligence that may affect their community or even add their own information and build upon it. If a cleared operator in a fusion center receives classified information they cannot declassify and share it with others. Even with an emphasis in our strategic documents on information sharing, “making information available to participants (people, processes, or systems),” there is still a tendency for agencies to limit their dissemination procedures with one another.[64]

Finally, in order to share information across the enterprise the government needs a network where all communities can collaborate. The solution for this requirement is a network that addresses "user needs and concerns at all levels….Just as important as the ability to share information is the willingness on the part of emergency managers to share information."[65] In 2004, DHS launched the Homeland Security Information Network (HSIN) as the primary means for the whole of government to share information. Unfortunately, DHS launched the system without studying the current environment and evaluating the systems used by the states and local communities.[66] They failed to consider the existence of other systems already used in the field by law enforcement, such as the Regional Information Sharing System (RISS), the Joint Regional Information Exchange System (JRIES), Law Enforcement Online (LEO), and an oversight mechanism incorporating these systems.[67] HSIN not only overlooked law enforcement systems, it failed to consider the more than fifteen different Emergency Operating Center (EOC) software options used in the states.[68] The oversights highlighted the fact that the system lacked integration with state EOCs.[69] In addition, studies indicated it had privacy issues, was not user friendly, and did not handle all events expected.[70] As a result of these pronounced shortcomings, DHS saw a requirement to establish a Homeland Security Information Network Advisory Committee (HSINAC).[71]

The HSINAC meets to gather information on the HSIN, and works to enhance and promote information sharing. The committee recognized its main obstacles to be "cross boundary and cultural issues…across jurisdictions, levels, and functions of government."[72] DHS acknowledges the existence of duplicative systems, but has no authority to enforce the use of HSIN. When questioned on law enforcement use of HSIN, the HSINAC admitted most of those agencies use LEO and RISS systems, and there would not be a change for the next few years.[73] Law enforcement‘s concern with HSIN was information overload with duplicative systems, and the need for DOJ and DHS to work together to eliminate competing systems for state and local users.[74] The primary DoD HSIN user, the National Guard, only posts to HSIN when it is approved by leadership, due to authentication, security concerns, and systems access.[75] These limiting factors of the HSIN challenge the preparedness of the nation to share intelligence and respond to a natural or manmade disaster.

Conclusion

Since the terrorist events of 2001 and Hurricane Katrina in 2005, the Federal Government focused efforts "aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation".[76] National preparedness not only involves response but a whole of government collaboration focused on "prevention, protection, mitigation, response, and recovery."[77] USNORTHCOM plans to train and equip smaller, more responsive units, which are more closely tied to the civil agencies they support. While the government is better prepared for natural and man-made disasters, it still lacks the information and intelligence sharing capability needed to prevent and respond to these events. There is still a substantial gap between the intelligence community and DHS, and their ability to collaborate with local law enforcement and fusion centers in the states. Incidents begin and end locally, but to achieve true success there is a need to involve "multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines."[78] There is a "seam of uncertainty" in the response enterprise, but it appears to be in collaboration, not in mission overlap. In the past ten years the government identified and closed seams in response and recovery by establishing DHS, USNORTHCOM, and their associated units. The remaining seam involves our information sharing capacity and collaboration.

Endnotes

[1] U.S. Joint Chiefs of Staff, *Homeland Defense and Civil Support Joint Operating Concept* (Washington, DC: U.S. Joint Chiefs of Staff, October 01, 2007), 2.

[2] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 18.

[3] Scott Pelley, "Fighting Terrorism in New York City," September 25, 2011, CBS News, streaming video, 14:21, http://www.cbsnews.com/video/watch/?id=7382308n&tag=contentBody;storyMediaBox (accessed October 18, 2011).

[4] Obama, *National Security Strategy,* 18.

[5] Ibid.,19.

[6] Ibid.,18-19.

[7] Obama, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: The White House, March 30, 2011), 1.

[8] Ibid., 2.

[9] Ibid., 3.

[10] Janet Napolitano, *Quadrennial Homeland Security Review Report* (Washington, DC: U.S. Department of Homeland Security**,** February 2010), viii.

[11] Ibid., ix.

[12] Ibid., 31.

[13] Ibid., 31.

[14] Ibid., 34.

[15] Ibid., 39.

[16] George W. Bush, *Homeland Security Presidential Directive/HSPD-5* (Washington, DC: The White House, February 2003), 1.

[17] Ibid., 2.

[18] Napolitano, *Quadrennial Homeland Security Review Report*, 72-73.

[19] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 18.

[20] Ibid.,19.

[21] Christine Le Jeune, “Consequence Management: Steps in the Right Direction?”, *Institute of Land Warfare*, September 8, 2010) 4.

[22] U.S. Government Accountability Office, *Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11,* (Washington, DC: U.S. Government Accountability Office, September 2011), 2.

[23] Michael Chertoff, *National Incident Management System* (Washington, DC: December 2008), 6.

[24] Ibid.

[25] US Department of Homeland Security, *National Response Framework* (Washington, DC: January 2008), 1.

[26] Ibid., 57.

[27] U.S. Joint Chiefs of Staff, *Homeland Defense*, (Washington, DC: U.S. Joint Chiefs of Staff, July 12, 2007), VII-5.

[28] U.S. Joint Chiefs of Staff, JP 3-28 *Civil Support*, (Washington, DC: U.S. Joint Chiefs of Staff, September 14, 2007), II-21-22.

[29] U.S. Joint Chiefs of Staff, JP 3-41 Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management, (Washington, DC: U.S. Joint Chiefs of Staff, October 2, 2006), II-7.

[30] Federal Emergency Management Agency Home Page, http://www.fema.gov/, (accessed 14 December 2011).

[31] Ibid.

[32] Gates, *Quadrennial Defense Review, 19.*

[33] Steve Cichocki, “*CBRN Response Enterprise Smartbook*,” briefing slides, United States Army Northern Command, December 2011.

[34] National Guard Home Page, http://www.ng.mil/features/HomelandDefense/cst/factsheet.html, (accessed December 14, 2011).

[35] Cichocki, “*CBRN Response Enterprise Smartbook”*

[36] Ibid.

[37] General Charles H. Jacoby, Commander, USNORTHCOM, "USNORTHCOM CONPLAN, CBRN Response 3500-11," Peterson Air Force Base, CO, United States Northern Command, August 17, 2011, 16.

[38] *Emergency Management Assistance Compact*, Public Law 104-321, 104th Cong., 2nd sess. (October 19, 1996).

[39] Jacoby, "USNORTHCOM CONPLAN, CBRN Response 3500-11," A-5.

[40] Ibid., A-3.

[41] Ibid., 22.

[42] Ibid., 3.

[43] Ibid., 18.

[44] Steve Cichocki, "USNORTHCOM CBRN Response Enterprise Update To Senior Steering Group," briefing slides, Peterson Air Force Base, CO, United States Northern Command, September 23, 2011.

[45] Ibid.

[46] US Department of Homeland Security, *National Response Framework*, 10.

[47] Ibid., 8.

[48] Ibid., 40.

[49] Ibid., 41.

[50] Ibid., 42.

[51] Chertoff, *National Incident Management System,* 23.

[52] Napolitano, *Quadrennial Homeland Security Review Report*, 34.

[53] James Burch, "The Domestic Intelligence Gap: Progress Since 9/11?," Homeland Security Affairs*,* Supplement no. 2 (2008): 9.

[54] Ibid., 10.

[55] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* 86.4 (Jul/Aug 2007): 3.

[56] Ibid., 3.

[57] Ibid., 4.

[58] Kevin D. Eack, “State and Local Fusion Centers: Emerging Trends and Issues,” *Homeland Security Affairs*, Supplement no.2 (2008): 2.

[59] Ibid., 1.

[60] Ibid., 2.

[61] Burch, “The Domestic Intelligence Gap: Progress Since 9/11?,” 13.

[62] Ibid.

[63] Ibid.

[64] Ibid., 14.

[65] Christopher Voss, *Connecting Our Nation’s Crisis Information Management Systems*, Thesis, (Monterey, CA: Naval Post Graduate School, December 2008), 2.

[66] Ibid., xvi.

[67] Burch, “The Domestic Intelligence Gap: Progress Since 9/11?,” 17.

[68] Voss, *Connecting Our Nation’s Crisis Information Management Systems*, 11.

[69] Ibid., 18.

[70] Ibid.

[71] Ibid., 3.

[72] U.S. Department of Homeland Security, *Final Report: Homeland Security Information Network Advisory Committee Meeting*, (Washington, DC: U.S. Department of Homeland Security, March 27, 2009), 5.

[73] Ibid., 15.

[74] Ibid., 21.

[75] Ibid., 26.

[76] Barack Obama, *Presidential Policy Directive 8: National Preparedness*, (Washington, DC: The White House, March 2011), 1.

[77] Ibid., 3.

[78] Voss, *Connecting Our Nation’s Crisis Information Management Systems*, 56.